AI-Enabled Ransomware Investigation Service Definition

Document title	AI-Enabled Ransomware Investigation Service Definition		
Reference No.	IF-SER-005	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Holly Jackson, Cyber Manager		
Issue date	23/01/2026		

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial draft	07/01/2026
0.2	Holly Jackson	Review and amendment	23/01/2026
1.0	Lisa Washer	Final review and publish	23/01/2026

Correlation Chart

Clause	FSR Code of Practice v2	ISO/IEC 17025:2017	ILAC-G19 :06/2022	ISO 9001:2015	ISO/IEC 27001:2022
Review of Requests, Tenders and Contracts	16	7.1	4.1, 4.7	8	4.2

Contents

1. AI-Enabled Ransomware Investigation Service

1.1 Service Overview

1.1.1 The AI-Enabled Ransomware Investigation Service provides specialist ransomware investigation support for organisations experiencing suspected or confirmed ransomware activity. The service leverages the Strand Intelligence Platform to apply AI-enabled automation to evidence collection, analysis, and structured investigation workflows, accelerating ransomware investigations while maintaining forensic integrity and expert oversight.

1.1.2 The service helps establish what occurred, how it occurred, and the impact, enabling informed decision-making, regulatory response, and recovery. Services are delivered by CREST- and SANS-accredited specialists operating as part of an NCSC Cyber Incident Response (CIR) accredited provider. This service is provided to clients on an ad-hoc consultancy basis and is engaged as required, with no pre-existing contract required.

1.2 Service Features

1.2.1 Below is a list of the core capabilities and characteristics of the AI-Enabled Ransomware Investigation service, describing what is delivered and how the service operates:

a) **Incident Scoping and Triage –** AI-assisted triage using endpoint-collected ransomware indicators to understand incident type, scope, severity, and priorities.

Digital Forensic Investigation – Endpoint-focused ransomware artefact analysis.

b) **Evidence Identification and Preservation -** Secure collection and handling of digital evidence in line with forensic best practice.

Timeline and Root Cause Analysis – Automated timeline reconstruction supported by AI correlation.

c) **User and Account Activity Analysis -** Review of user actions, credential misuse, and privilege escalation.

Malware and Artifact Analysis – AI-enabled ransomware family identification and execution analysis.

Log and Network Traffic Analysis – Endpoint-derived execution and persistence evidence.

d) **Impact and Data Exposure Assessment -** Determination of affected systems, data types, and potential data exfiltration.

e) Advisory Support for Containment and Recovery - Expert guidance to support effective containment, remediation planning, and recovery.

f) **AI-Enabled Investigation Workflows** – Automated, repeatable ransomware investigation workflows powered by the Strand Intelligence Platform, reducing manual effort and increasing consistency.

g) **Technical and Executive Reporting -** Clear, evidence-based reports suitable for technical teams, management, and regulators.

h) **Regulatory and Stakeholder Support -** Support for regulatory notification, audit response, and stakeholder communications.

Accredited Specialist Delivery - Investigations conducted by CREST- and SANS-accredited specialists operating under an NCSC CIR accredited provider.

2. Service Benefits

2.1.1 The AI-Enabled Ransomware Investigation Service provides organisations with timely, expert support to understand and respond effectively to Ransomware incidents. Key benefits include:

Faster investigations - Faster ransomware Investigation timelines through AI-enabled automation.

Workload reduction – Reduced analyst workload during ransomware incidents.

a) **Workflow efficiency** – Consistent, repeatable investigation outcomes across endpoints.

b) **Rapid Clarity on Incidents -** Establishes what occurred, how the incident unfolded, and the full scope of impact.

c) **Reduced Business Disruption -** Supports effective containment and recovery to minimise operational downtime.

d) **Evidence-Based Decision Making -** Provides reliable forensic findings to inform response, recovery, and escalation decisions.

e) **Regulatory and Legal Confidence -** Supports compliance with regulatory, contractual, and reporting obligations.

f) **Preservation of Evidential Integrity -** Ensures evidence is handled in accordance with recognised forensic standards.

g) **Improved Risk Management -** Identifies root causes and control weaknesses to reduce the likelihood of recurrence.

h) **Executive and Stakeholder Assurance -** Delivers clear reporting to support board-level, customer, and regulator confidence.

i) **Independent Expert Support -** Provides objective analysis delivered by accredited specialists independent of internal teams.

j) **Improved Incident Response Maturity -** Informs enhancements to incident response processes, controls, and organisational readiness.

k) **Trusted Accredited Delivery -** Delivered by CREST- and SANS-accredited specialists operating as an NCSC CIR accredited provider.

3. Scope of Service

3.1 In-Scope of Service

3.1.1 The AI-Enabled Ransomware Service is focused specifically on ransomware and suspected ransomware activity and does not provide general cyber incident investigation unless separately agreed. The scope of the service includes the following activities:

a) **Ransomware Incident Scoping and AI-Assisted Triage -** Initial assessment to confirm whether ransomware activity has occurred or is suspected. This includes AI-assisted triage using endpoint-derived indicators to identify ransomware behaviours, affected hosts, likely infection vectors, and investigation priorities. Early scoping informs containment decisions and investigation depth.

b) **AI-Enabled Endpoint Evidence Collection -** Deployment and use of the Strand Intelligence Platform's lightweight endpoint agent to collect relevant system-level and forensic artefacts from in-scope devices. This includes collection of execution artefacts, process activity, file system changes, persistence mechanisms, and other ransomware-relevant indicators, performed in a controlled and auditable manner.

c) **Automated Ransomware Investigation Workflows -** Execution of structured, AI-enabled investigation workflows designed specifically for ransomware analysis. These workflows automate evidence correlation, artefact enrichment, and investigation steps to accelerate analysis, reduce manual effort, and ensure consistent investigation outcomes across multiple endpoints.

d) **Ransomware Family and Variant Identification -** AI-enabled analysis to identify likely ransomware families or variants based on observed behaviours, artefacts, and execution patterns. Findings are validated and contextualised by specialist analysts to support response, containment, and external reporting.

e) **Timeline Reconstruction and Attack Path Analysis -** Automated and expert-led reconstruction of ransomware activity timelines, detailing key events from initial access through execution and impact. This supports understanding of how the ransomware was deployed and how it progressed across affected endpoints.

f) **Impact and Encryption Assessment** - Assessment of the impact of ransomware activity, including identification of affected systems, encrypted files, disrupted services, and operational impact. This may include analysis of encryption scope, file types impacted, and evidence of partial or failed encryption attempts.

g) **Data Exposure and Exfiltration Indicators** - Assessment for indicators of data access or exfiltration commonly associated with ransomware operations, based on endpoint evidence and observable artefacts. This activity is limited to ransomware-relevant indicators and does not constitute full network-wide exfiltration analysis unless separately agreed.

h) **Advisory Support for Containment and Recovery**- Provision of expert advice informed by investigation findings to support containment actions, recovery planning, and decision-making. This includes guidance on isolating affected systems, validating eradication steps, and understanding residual risk following ransomware activity.

i) **Reporting and Investigation Outputs** - Delivery of technical and executive-level reports documenting ransomware investigation scope, methods, findings, timelines, and conclusions. Reports clearly distinguish AI-enabled automated findings from analyst interpretation and include known limitations.

j) **Legal and Regulatory Support -** The AI-Enabled Ransomware Service includes advisory support to assist organisations in meeting legal and regulatory requirements arising from a ransomware incident. This includes support for legally privileged reporting where engagement is coordinated through external legal counsel, assistance to Data Protection Officers (DPOs) in assessing personal data impact and regulatory notification obligations, and preparation of investigation outputs suitable for legal review. Where required, suitably qualified specialists may provide expert witness services, including written statements and court or tribunal testimony, subject to separate agreement.

3.2 Out-of-scope activities

3.2.1 The following activities are not included as part of the standard AI-Enabled Ransomware Investigation Service scope. However, the organisation can provide support for these activities through additional services or established partner arrangements, subject to separate agreement:

a) Investigation of non-ransomware cyber incidents

b) Live system remediation, rebuild, or recovery activities

c) Provision of legal advice or legal representation

d) Continuous monitoring, managed detection, or managed response services

e) Investigation of third-party systems without appropriate authorisation

3.3 Assumptions, Constraints and Dependencies

3.3.1 Delivery of the AI-Enabled Ransomware Investigation Service is subject to the following assumptions, constraints, and dependencies, which influence scope, timelines, and outcomes.

a) **Client Authority and Access** - It is assumed that the organisation has the legal authority to grant access to in-scope systems, data, and users. Investigation activities are constrained to systems and information explicitly authorised by the organisation.

b) **Availability and Accuracy of Information** - The effectiveness of the investigation depends on the accuracy, completeness, and availability of information, logs, and documentation provided. Limitations in data retention, logging, or system visibility may restrict findings.

c) **Timely Client Engagement** - Progress and timelines depend on timely engagement from nominated client contacts, including system owners, subject matter experts, and decision-makers.

d) **Third-Party Dependencies** - Investigations involving cloud providers, suppliers, or external platforms rely on third-party cooperation and legal processes, which may introduce delays or limit access to evidence.

e) **Point-in-Time Assessment** - Findings represent a snapshot based on the evidence available during the investigation and may not identify all historical activity or enable definitive attribution.

f) **Operational Constraints** - Investigation activities are conducted to minimise business disruption; certain actions may be limited by operational, safety, or business continuity requirements.

g) **Resource Availability** - Delivery is subject to specialist availability and agreed engagement terms, including scheduling and priority requirements.

4. Onboarding

4.1 Live Incident Onboarding

4.1.1 Onboarding commences immediately upon service initiation and is designed to enable rapid, structured engagement during a ransomware incident. At the outset, a dedicated incident response team is established and aligned to the organisation. This team consists of an Account Manager as the primary commercial and engagement point of contact, an Incident Manager responsible for overall coordination and incident governance, and a Cyber Incident Response (CIR) Specialist responsible for technical investigation and analysis.

4.1.2 During onboarding, the incident context is captured, and a preliminary timeline of events is developed to document key occurrences from initial detection to engagement. Any actions taken prior to service commencement are identified and recorded to inform investigation planning and preserve evidential integrity. Scope, objectives, and legal authorisation to investigate are confirmed, and key stakeholders, escalation paths, and reporting requirements are agreed.

4.1.3 Communication frequency and methods, including regular status updates, escalation notifications, and reporting cadence, are defined and agreed at the outset to ensure clear, consistent engagement throughout the investigation. Access requirements, constraints, and dependencies are documented, and coordination with legal, compliance, or third-party providers is initiated where required. Onboarding ensures clarity of roles, responsibilities, and next steps, enabling effective and timely investigation activities.

4.2 Pro-active deployment Onboarding

4.2.1 In addition to incident-driven onboarding, the AI-Enabled Ransomware Investigation Service may be deployed proactively in a non-incident context to support preparedness, early detection, and rapid investigation readiness.

4.2.2 Where the service is deployed proactively, onboarding includes coordination with the organisation to plan and execute controlled deployment of the Strand Intelligence Platform endpoint agent across agreed systems. This deployment is conducted without initiating an active investigation and is designed to enable rapid activation of AI-enabled investigation workflows should ransomware activity be suspected in the future.

4.2.3 During proactive onboarding, the following activities are completed:

a) Confirmation of deployment scope, including systems, user groups, and environments

b) Validation of technical prerequisites, connectivity, and security controls

c) Configuration of access controls, roles, and permissions within the Strand platform

d) Agreement of activation triggers, escalation paths, and investigation initiation procedures

e) Documentation of deployment status and readiness

4.2.4 Proactive deployment does not include continuous monitoring or managed detection and does not generate investigation outputs unless an investigation is formally initiated. Activation of investigation workflows remains subject to explicit client authorisation in line with agreed procedures.

4.2.5 This approach enables faster response and reduced investigative overhead during ransomware incidents while maintaining clear governance and control.

5. Service Delivery Model

5.1.1 The AI-Enabled Ransomware Investigation Service is delivered using a structured and flexible engagement approach designed to support organisations during suspected or confirmed Ransomware incidents. Delivery is tailored to the nature, severity, and complexity of the incident while following recognised incident response and forensic investigation practices.

5.2 Engagement Approach

5.2.1 The service combines AI-enabled automated investigation workflows delivered through the Strand Intelligence Platform with expert forensic oversight, enabling rapid, scalable ransomware investigations without sacrificing evidential quality.

5.2.2 AI-enabled automation is used to accelerate and standardise investigation activities and does not replace expert analysis, decision-making, or reporting.

5.2.3 Service delivery begins upon formal engagement approval and completion of onboarding activities. A dedicated incident response team is assigned, comprising an Account Manager, Incident Manager, and Cyber Incident Response (CIR) Specialist. The engagement is led by the Incident Manager, who coordinates activities, manages priorities, and acts as the primary operational point of contact. The approach is collaborative and evidence-led, with regular communication and agreed reporting throughout the engagement.

5.3 Delivery Phases

5.3.1 The service is typically delivered across the following phases:

a) **Initial Triage and Scoping -** Rapid assessment to confirm incident type, scope, severity, and immediate priorities. This phase includes review of initial indicators, validation of incident status, and confirmation of investigation objectives.

b) **Automated and Expert-Led Ransomware Analysis -** Detailed forensic investigation of in-scope systems, accounts, and data. Activities may include endpoint, server, network, and log analysis, evidence preservation, and reconstruction of attacker activity.

c) **Impact Assessment and Advisory Support -** Assessment of business, operational, and data impact, including potential regulatory considerations. Advisory support is provided to inform containment, remediation planning, and recovery decisions.

d) **Reporting and Close-Out -** Delivery of technical and executive reports detailing findings, timelines, conclusions, and recommendations. A close-out discussion is held to review outcomes and next steps.

5.4 Typical Timelines

5.4.1 Timelines vary depending on incident severity, number of affected endpoints, data availability, and whether the Strand Intelligence Platform has been deployed proactively prior to an incident. The use of AI-enabled automated investigation workflows typically reduces investigation timeframes compared to traditional manual approaches.

5.5 Proactive Deployment (Non-Incident Scenario)

5.5.1 Where the service is onboarded proactively, initial deployment and readiness activities are typically completed within 2–5 business days, subject to endpoint volume, access approvals, and technical prerequisites. This includes agent deployment to agreed systems, validation of connectivity, and confirmation of investigation activation procedures.

5.5.2 Once deployed, the platform remains in a ready state, enabling immediate activation of ransomware investigation workflows if required.

5.6 Incident-Driven Investigation Timelines

5.6.1 Following confirmation of engagement and authorisation, investigation timelines typically align to the severity of ransomware activity:

a) **Suspected Ransomware (1–2 days):** Initial triage, AI-enabled evidence collection, and validation to confirm or rule out ransomware activity on identified endpoints.
b) **Confirmed Ransomware – Limited Scope (2–4 days):** Automated investigation workflows executed across a limited number of endpoints to analyse execution, encryption activity, and initial impact.
c) **Confirmed Ransomware – Multi-Endpoint (4–7 days):** Expanded investigation across multiple endpoints, automated timeline reconstruction, ransomware family identification, and impact assessment.
d) **Major Ransomware Incident (7–14+ days):** Large-scale or complex incidents involving widespread endpoint impact, regulatory considerations, or extended advisory support. Investigation duration depends on endpoint volume, organisational complexity, and external dependencies.

5.7 Delivery Modes

5.7.1 The service may be delivered remotely, on-site, or through a hybrid approach, depending on incident requirements, data sensitivity, and client preference. Remote delivery is used where secure access can be provided, while on-site support may be required for sensitive environments, evidence handling, or operational constraints.

6. Support Model

6.1.1 The AI-Enabled Ransomware Investigation Service is supported through defined levels of engagement to ensure appropriate coverage based on incident severity and client requirements. Support levels, hours of operation, and escalation arrangements are agreed at the outset of the engagement and may be adjusted as the incident evolves.

6.2 Standard Support

6.2.1 Standard support is provided during business hours and includes investigation activities, incident coordination, and regular status updates. The service is delivered by a dedicated Cyber Incident Response (CIR) Specialist, overseen by an Incident Manager**,** with an Account Manager providing engagement oversight. Standard support includes agreed reporting and access to subject matter expertise as required.

6.3 Enhanced Support

6.3.1 Enhanced support may be provided for higher-severity incidents or where extended coverage is required. This may include out-of-hours or weekend support, accelerated investigation activities, increased specialist resource allocation, and more frequent status updates. Enhanced support is delivered subject to availability and separate agreement.

6.4 Escalation Paths

6.4.1 Operational escalation is managed by the Incident Manager, who coordinates resources and resolves issues impacting investigation progress. Strategic or commercial escalation is managed by the Account Manager. Escalation to senior technical specialists or management occurs where incident severity, regulatory risk, or complexity increases.

6.5 Optional Support Services

6.5.1 In addition to the core investigation service, optional specialist support services may be provided subject to separate agreement. These include executive-level briefings, regulatory-focused reporting, extended post-incident monitoring, expert witness support, and follow-on incident response or remediation advisory services. Further specialist services may also be provided to support broader incident response and recovery activities, including eDiscovery services to support Data Protection Officers (DPOs) and data breach analysis, malware analysis, threat hunting, penetration testing, and wider cyber security consultancy services. Services may be delivered directly or through established partner arrangements, depending on scope and requirements.

7. Service Level Agreements

7.1.1 The following service levels describe indicative performance targets for the AI-Enabled Ransomware Investigation Service. These service levels are provided for guidance only and do not constitute guaranteed commitments unless expressly agreed in writing.

7.1.2 Where a pre-existing contract or retainer agreement is in place, including an Incident Response (IR) Retainer, the service levels and SLAs defined within that agreement shall apply and take precedence over the indicative service levels outlined below.

7.2 Response time

7.2.1 Initial response is provided following confirmation of engagement and receipt of appropriate authorisation. For Ransomware incidents, initial engagement typically occurs within 4–8 business hours.

7.3 Investigation Commencement

7.3.1 Investigation activities commence once scope, access, and legal authorisation are confirmed. For urgent incidents, investigative work typically begins within 24 hours of engagement approval.

7.4 Availability Windows

7.4.1 Standard service delivery is provided during business hours, with enhanced or out-of-hours support available by agreement. Availability may be extended for high-severity incidents, subject to resource availability and agreed terms.

7.5 Delivery timeframe

7.5.1 Investigation duration varies depending on incident complexity, system scope, and data availability. Indicative investigations may range from several days to multiple weeks

7.6 Reporting Commitments

7.6.1 Interim status updates are provided at an agreed frequency. Final technical and executive reports are typically delivered within 5–10 business days of investigation completion, subject to scope and review requirements.

8. Roles and Responsibilities

8.1.1 The following roles are defined to ensure effective governance, delivery, and communication throughout the AI-Enabled Ransomware Investigation Service engagement.

8.2 Account Manager

8.2.1 Acts as the primary commercial and engagement contact for the organisation. Responsible for contract management, service coordination, and strategic escalation. Ensures the service is delivered in line with agreed scope and expectations.

8.3 Incident Manager

8.3.1 Provides overall operational leadership for the investigation. Responsible for incident coordination, prioritisation, decision-making, escalation management, and communication oversight. Acts as the primary operational point of contact throughout the engagement.

8.4 Cyber Incident Response (CIR) Specialist

8.4.1 Responsible for the technical investigation and forensic analysis. Conducts evidence collection, analysis, and documentation in accordance with recognised forensic standards. Provides expert input to support containment, remediation planning, and reporting.

8.5 Client Incident Lead

8.5.1 Acts as the organisation's primary point of contact for the investigation. Coordinates internal stakeholders, facilitates access to systems and information, and supports decision-making and escalation activities.

8.6 Client Stakeholders and Subject Matter Experts

8.6.1 Provide system access, technical knowledge, and operational context required to support investigation activities and validate findings.

8.7 Service RACI Matrix

8.7.1 The following RACI matrix defines roles and responsibilities for the delivery of the AI-Enabled Ransomware Investigation Service. It clarifies accountability and ownership across key activities to ensure effective governance, communication, and execution throughout the engagement. The matrix identifies who is Responsible, Accountable, Consulted, and Informed for each activity, supporting clear decision-making, efficient escalation, and coordinated incident response.

Activity / Task	*Account Manager*	*Incident Manager*	*Ransomware Investigation Specialist*	*Client Incident Lead*	*Client SMEs*
Engagement initiation & onboarding	R	A	C	C	I
Proactive platform deployment planning	C	A	R	C	I
Endpoint agent deployment	I	C	C	A	R
Platform access & role configuration	I	A	R	C	I
Investigation activation authorisation	I	A	C	R	I
Ransomware scoping & AI-assisted triage	I	A	R	C	C
AI-enabled evidence collection	I	C	R	I	I
Automated investigation workflow execution	I	C	R	I	I
Ransomware behaviour & family analysis	I	C	R	I	C
Timeline reconstruction & impact assessment	I	A	R	C	C
Data exposure indicator assessment	I	A	R	C	C

Advisory support (containment & recovery)	I	A	R	C	C
Status updates & stakeholder communications	C	A	R	C	I
Critical finding escalation	I	A	R	C	I
Reporting (technical & executive)	I	A	R	C	I
Regulatory / insurer support (if required)	C	A	R	C	I
Service close-out & offboarding	R	A	C	C	I

9. Technical Requirements

9.1.1 Delivery of the AI-Enabled Ransomware Investigation Service requires appropriate technical access, information, and resources to enable effective investigation activities. The following requirements apply and are confirmed during onboarding.

a) **Authorisation and Access -** Written authorisation must be provided confirming the organisation's approval for investigation activities. Secure access to in-scope systems, applications, networks, cloud environments, and data sources is required, including administrative or read-only access as appropriate.

b) **Endpoint Agent Deployment Authorisation** - The client must provide written authorisation to deploy the Strand Intelligence Platform lightweight endpoint agent to agreed systems. Deployment may be performed proactively in a non-incident scenario and enables rapid activation of ransomware investigation workflows when required.

c) **Supported Endpoint Platforms** - The service requires deployment to supported endpoint operating systems and versions. Platform compatibility is confirmed during onboarding to ensure reliable evidence collection and consistent investigation outcomes across in-scope devices.

Network Connectivity and Access – Where possible Endpoints must be able to establish secure outbound connectivity to the Strand Intelligence Platform using approved network paths. Required ports, protocols, and destinations are confirmed in advance to ensure reliable operation without introducing unnecessary network exposure. Where network connectivity is unavailable, restricted, or intentionally isolated, the Strand Intelligence Platform endpoint agent supports offline operation. The agent may be securely downloaded and deployed to endpoints using offline distribution methods, including removable media or other client-approved transfer mechanisms. In offline scenarios, evidence collection and investigation workflows execute locally on the endpoint, with collected artefacts securely packaged for manual upload to the Strand platform.

d) **Security Controls and Allowlisting -** Where endpoint protection, application control, or network security tools are in place, appropriate allowlisting must be configured to permit authorised Strand agent operation. This ensures evidence collection and investigation workflows can execute without interference.

e) **Data Collection Scope** - Evidence collection is limited to artefacts relevant to ransomware investigation objectives. Data collection scope is defined during onboarding to support forensic analysis while minimising unnecessary data access or processing.

f) **Logging and Data Availability -** Access to relevant system, application, security, and network logs is required. The scope and depth of findings depend on log availability, retention periods, and data quality.

g) **System and Environment Information -** Provision of relevant technical documentation, such as network diagrams, asset inventories, system architecture, identity and access models, and security tooling in use, to support investigation planning and analysis.

h) **User and Stakeholder Availability -** Availability of system owners, administrators, and subject matter experts to support access provisioning, clarify system behaviour, and validate findings.

i) **Secure Communications -** Use of secure communication channels for information exchange, including file transfer and reporting, to protect sensitive investigation data.

j) **Third-Party Platforms -** Access to cloud providers, software vendors, or external platforms may require additional approvals or legal processes and may impact investigation timelines

10. Exit and Offboarding

10.1.1 The AI-Enabled Ransomware Investigation Service concludes once all agreed investigation activities have been completed and final deliverables have been provided. Service closure is managed in a controlled manner to ensure clarity of outcomes, secure handling of information, and effective knowledge transfer.

10.2 Final Deliverables

10.2.1 At service completion, agreed outputs are delivered to the organisation. This typically includes technical and executive reports detailing investigation scope, findings, timelines, conclusions, and recommendations. Where applicable, additional deliverables such as evidence inventories, indicators of compromise, or expert statements are provided.

10.3 Knowledge Transfer and Close-Out

10.3.1 A close-out meeting may be held to review findings, explain conclusions, and discuss recommended next steps. This session supports knowledge transfer to relevant stakeholders, including IT, security, legal, and management teams, and provides an opportunity to address questions and clarify outcomes.

10.4 Data Handling and Retention

10.4.1 All investigation data and evidence are handled in accordance with agreed data handling, confidentiality, and retention requirements. Data is securely stored during the engagement and, following service completion, is either securely transferred to the organisation or retained for an agreed period before secure disposal, in line with contractual and regulatory obligations.

10.5 Service Closure

10.5.1 The service is formally closed once deliverables are accepted and offboarding activities are completed. Any further support required beyond service closure is subject to a new or extended engagement.

*****END OF DOCUMENT*****